Government Smart Card Interoperability Specification v2.1 (NISTIR 6887, 2003 Edition) Virtual Card Edge Interface File System Cards

Conformance Test Assertions

DRAFT

Alan Goldfine

April 12, 2004

This document contains the conformance test assertions for each of the APDUs comprising the File System Virtual Card Edge Interface (VCEI) of version 2.1 of the Government Smart Card Interoperability Specification (GSC-IS), as contained in NIST Interagency Report 6887, 2003 Edition.

The 13 sections of this document correspond to the 13 APDUs in the VCEI, as specified in Section 5.1. The test assertions for each of the APDUs are numbered in the form X.Y, where X is the APDU number, and Y is the number of the assertion for that APDU. Thus, 6.7 is the number given to assertion 7 for APDU 6 (SELECT MASTER FILE).

1. GET RESPONSE

CLA	00
INS	C0
P1	00
P2	00
L_c	empty
Data Field	empty
L_e	number of bytes to read in response

References:

1. GSC-IS 5.1.1.1.

Note: It is assumed that GET RESPONSE is only used in environments using the T=0 communications protocol.

Starting State for Each Assertion:

1. A card that claims to implement the GSC-IS, Version 2.1, is in a reader.

2. The immediately preceding APDU has indicated that a block of L bytes of additional data is available to be read.

Assertion 1.1

Purpose: To test GET RESPONSE using valid parameters, with the number of bytes specified to be read equal to the maximum available.

Scenario:

1. L_e == L.

2. A GET RESPONSE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 90 00
   - Response Data Field == the string of bytes, of length L_e, that is read.

Assertion 1.2

Purpose: To test GET RESPONSE using valid parameters, where the number of bytes specified to be read is less than the maximum available.

Scenario:

1. L_e < L.

2. A GET RESPONSE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 61 XX, where XX is L - L_e

- Response Data Field == the string of bytes, of length L, that is read.

Assertion 1.3

Purpose: To test GET RESPONSE where part of the returned data may be corrupted.

The assertion is not testable.

Assertion 1.4

Purpose: To test GET RESPONSE where the number of bytes specified to be read is greater than the maximum available.

Scenario:

1. L_e > L.

2. A GET RESPONSE APDU is issued

Expected Results:

1. The APDU returns
    - SW1 SW2 == 67 00 or 6C XX.

Assertion 1.5

Purpose: To test GET RESPONSE using invalid parameters P1-P2.

Scenario:

1. L_e == L.

2. At least one of P1 or P2 is /= 0.

3. A GET RESPONSE APDU is issued.

Expected Results:

1. The APDU returns
    - SW1 SW2 == 6A 86.

2. READ BINARY

CLA	00
INS	B0
P1	off/H
P2	off/L
L_c	empty
Data Field	empty
L_e	number of bytes to read

Note: P1P2 will be used to represent the 2 byte file offset formed by combining P1 and P2.

References:

1. GSC-IS 5.1.1.2.

Starting State for Each Assertion:

1. A card that claims to implement the GSC-IS, Version 2.1, is in a reader.

Assertion 2.1

Purpose: To test READ BINARY using valid parameters.

Scenario:

1. An Elementary File on the card is currently selected.

2. P1P2 represents an offset that is within the current bounds of the selected EF.

3. L_e is a number such that the offset L_e + P1P2 is within the current bounds of the selected EF.

4. A READ BINARY APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 90 00 or 61 L_e
   - Response Data Field == the string of bytes, of length L_e, that is read.

Note: For systems using the T=0 communications protocol, the 61 XX response is required by ISO 7816-4.

Assertion 2.2

Purpose: To test READ BINARY where part of the returned data may be corrupted.

The assertion is not testable.

Assertion 2.3

Purpose: To test READ BINARY where the end of the file is reached before the specified number of bytes has been read.

Scenario:

1. An Elementary File on the card is currently selected.
2. P1P2 represents an offset that is within the current bounds of the selected EF.
3. L_e is a number such that the offset L_e + P1P2 is outside the current bounds of the selected EF.
4. A READ BINARY APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 62 82, 67 00, 6C XX, or 61 00.

Assertion 2.4

Purpose: To test READ BINARY where the command is incompatible with the file structure.

This situation cannot occur in the context of READ BINARY. The assertion is not testable.

Assertion 2.5

Purpose: To test READ BINARY where the security status of the selected file is not satisfied.

Scenario:

1. An Elementary File on the card is currently selected.
2. P1P2 represents an offset that is within the current bounds of the selected EF.
3. L_e is a number such that the offset L_e + P1P2 is within the current bounds of the selected EF.
4. The current application has not satisfied the security status of the selected EF.
5. A READ BINARY APDU is issued

Expected Results:

1. The APDU returns
   - SW1 SW2 == 69 82.

Assertion 2.6

Purpose: To test READ BINARY with no selected EF.

Scenario:

1. No elementary file on the card is currently selected.

2. P1P2 == 0.

3. L_e == 0.

4. A READ BINARY APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 69 86 or 6A 82.

Assertion 2.7

Purpose: To test READ BINARY where the function is not supported.

The assertion is not testable.

Assertion 2.8

Purpose: To test READ BINARY using an offset outside the selected file.

Scenario:

1. An Elementary File on the card is currently selected.

2. P1P2 represents an offset that is outside the current bounds of the selected EF.

3. L_e == 0.

4. A READ BINARY APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 6B 00.

3. SELECT DF

CLA	00
INS	A4
P1	01
P2	00 for response required 0C for no response required
L_c	02
Data Field	File ID of the dedicated file to be selected
L_e	Number of bytes expected in the data field of the response to the command *(Is this always correct? If P2 == 0C, shouldn't L_e be empty?)*

References:

1. GSC-IS 5.1.1.3.

Starting State for Each Assertion:

1. A card that claims to implement the GSC-IS, Version 2.1, is in a reader.

2. A dedicated file is currently selected.

Assertion 3.1

Purpose: To test SELECT DF using valid parameters (no response required).

Scenario:

1. P2 == 0C.

2. Data Field == the file ID of a dedicated file that is contained in the currently selected dedicated file.

3. A SELECT DF APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 90 00

   or
   - SW1 SW2 == 61 XX.

Note: We allow for 61 XX, because some systems may generate a response even if none is requested.

2. The specified child dedicated file is selected.

Assertion 3.2

Purpose: To test SELECT DF using valid parameters (response required).

Scenario:

1. P2 == 00.

2. Data Field == the file ID of a dedicated file that is contained in the currently selected dedicated file.

3. A SELECT DF APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 90 00 or 61 L_e
   - Response Data Field == a string of bytes of length L_e representing the File Control Information.

Note: For systems using the T=0 communications protocol, the 61 XX response is required by ISO 7816-4.

2. The specified child dedicated file is selected.

Assertion 3.3

Purpose: To test SELECT DF using valid parameters (no response required) and a card in which the selected file has been deactivated. *(does "deactivated" refer to the currently selected file or to the file to be selected?)*

(Is this assertion relevant enough to the GSC-IS to require testing?)

Scenario:

1. P2 == 00.

2. Data Field == the file ID of a dedicated file that is contained in the currently selected dedicated file. This file is currently deactivated.

3. A SELECT DF APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 62 83.

Assertion 3.4

Purpose: To test SELECT DF using valid parameters (no response required) and a card in which the FCI is not formatted according to ISO 7816-4 Section 5.1.5.

(Is this assertion relevant enough to the GSC-IS to require testing?)

Scenario:

1. The FCI is not formatted according to ISO 7816-4 Section 5.1.5.

2. P2 == 0C.

3. Data Field == the file ID of a dedicated file that is contained in the currently selected dedicated file.

4. A SELECT DF APDU is issued.

Expected Results:

1. The APDU returns

- SW1 SW2 == 62 84.

Assertion 3.5

Purpose: To test SELECT DF where the function is not supported.

The assertion is not testable.

Assertion 3.6

Purpose: To test SELECT DF using valid parameters (no response required) and a card that does not contain a file identified by the specified file ID *Note: The test assertions for Version 2 of the Card Edge Test Suite will also include the case for which response is required).*

Scenario:

1. P2 == 0C.
2. Data Field == an ID that does not represent a file contained in the currently selected dedicated file.
3. A SELECT DF APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2== 6A 82.

Assertion 3.7

Purpose: To test SELECT DF using invalid parameters P1-P2.

Scenario:

1. At least one of the following is true:
   - P1 /= 00, 01, 02, or 03
   - P2 /= 00 or 0C.
2. Data Field == the file ID of a dedicated file that is contained in the currently selected dedicated file.
3. A SELECT DF APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 6A 86.

Assertion 3.8

Purpose: To test SELECT DF using an L_c inconsistent with P1-P2 (no response required) *Note: The test assertions for Version 2 of the Card Edge Test Suite will also include the case for which response is required).*

Scenario:

1. P2 == 0C.

2. L_c /= 02.

3. Data Field == the file ID of a dedicated file that is contained in the currently selected dedicated file.

4. A SELECT DF APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 6A 87.

4. SELECT EF UNDER SELECTED DF

CLA	00
INS	A4
P1	02
P2	00 for response required 0C for no response required
L_c	02
Data Field	File ID of the elementary file to be selected
L_e	Number of bytes expected in the data field of the response to the command *(Is this always correct? If P2 == 0C, shouldn't L_e be empty?)*

References:

1. GSC-IS 5.1.1.3.1. *(should be 5.1.1.4)*

Starting State for Each Assertion:

1. A card that claims to implement the GSC-IS, Version 2.1, is in a reader.

2. A dedicated file is currently selected.

Assertion 4.1

Purpose: To test SELECT EF UNDER SELECTED DF using valid parameters (no response required).

Scenario:

1. P2 == 0C.

2. Data Field == the file ID of an elementary file that is contained in the currently selected dedicated file.

3. A SELECT EF UNDER SELECTED DF APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 90 00

   or
   - SW1 SW2 == 61 XX.

- *Note: We allow for 61 XX, because some systems may generate a response even if none is requested.*

2. The specified child elementary file is selected.

Assertion 4.2

Purpose: To test SELECT EF UNDER SELECTED DF using valid parameters (response required).

Scenario:

1. P2 == 00.

2. Data Field == the file ID of an elementary file that is contained in the currently selected dedicated file.

3. A SELECT EF UNDER SELECTED DF APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 90 00 or 61 L_e
   - Response Data Field == a string of bytes of length L_e representing the File Control Information.
   - *Note: For systems using the T=0 communications protocol, the 61 XX response is required by ISO 7816-4.*

2. The specified child elementary file is selected.

Assertion 4.3

Purpose: To test SELECT EF UNDER SELECTED DF using valid parameters (no response required) and a card in which the selected file has been deactivated. *(does "deactivated" refer to the currently selected file or to the file to be selected?)*

(Is this assertion relevant enough to the GSC-IS to require testing?)

Scenario:

1. P2 == 00.

2. Data Field == the file ID of an elementary file that is contained in the currently selected dedicated file. This file is currently deactivated.

3. A SELECT EF UNDER SELECTED DF APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 62 83.

Assertion 4.4

Purpose: To test SELECT EF UNDER SELECTED DF using valid parameters (no response required) and a card in which the FCI is not formatted according to ISO 7816-4 Section 5.1.5.

(Is this assertion relevant enough to the GSC-IS to require testing?)

Scenario:

1. The FCI is not formatted according to ISO 7816-4 Section 5.1.5.

2. P2 == 0C.

3. Data Field == the file ID of an elementary file that is contained in the currently selected dedicated file.

4. A SELECT EF UNDER SELECTED DF APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 62 84.

Assertion 4.5

Purpose: To test SELECT EF UNDER SELECTED DF where the function is not supported.

The assertion is not testable.

Assertion 4.6

Purpose: To test SELECT EF UNDER SELECTED DF using valid parameters (no response required) and a card that does not contain a file identified by the specified file ID. *Note: Future versions of the Card Edge Test Suite will also include the case for which response is required).*

Scenario:

1. P2 == 0C.

2. Data Field == an ID that does not represent a file contained in the currently selected dedicated file.

3. A SELECT EF UNDER SELECTED DF APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2== 6A 82.

Assertion 4.7

Purpose: To test SELECT EF UNDER SELECTED DF using invalid parameters P1-P2.

Scenario:

1. At least one of the following is true:
   - P1 /= 00, 01, 02, or 03
   - P2 /= 00 or 0C.

2. Data Field == the file ID of an elementary file that is contained in the currently selected dedicated file.

3. A SELECT EF UNDER SELECTED DF APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 6A 86.

Assertion 4.8

Purpose: To test SELECT EF UNDER SELECTED DF using an L_c inconsistent with P1-P2 (no response required) *Note: Future versions of the Card Edge Test Suite will also include the case for which response is required).*

Scenario:

1. P2 == 0C.
2. L_c /= 02.
3. Data Field == the file ID of an elementary file that is contained in the currently selected dedicated file.
4. A SELECT EF UNDER SELECTED DF APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 6A 87.

5. SELECT FILE

CLA	00
INS	A4
P1	00 Explicit selection with Data Field; Data field must contain a valid File Identifier 01 Select child DF of current DF; Data Field must contain a valid File Identifier *(Note: This case is not tested here. It is tested in section 3.)* 02 Select child EF of current DF; Data Field must contain a valid File Identifier *(Note: This case is not tested here. It is tested in section 4.)* 03 Select parent DF of current DF; empty Data Field
P2	00 for response required 0C for no response required
L_c	02
Data Field	File ID (empty for P1 == 03)
L_e	Empty *(Is this always correct? If P2 == 00. shouldn't L_e contain the maximum number of bytes expected in the data field of the response to the command?)*

References:
1. GSC-IS 5.1.1.4.

Starting State for Each Assertion:
1. A card that claims to implement the GSC-IS, Version 2.1, is in a reader.

Assertion 5.1

Purpose: To test SELECT FILE using valid parameters (explicit selection, no response required)

Scenario:
1. P1 == 00.

2. P2 == 0C.

3. Data Field == a valid file ID for a file on the card.

4. A SELECT FILE APDU is issued.

Expected Results:
1. The APDU returns
    - SW1 SW2 == 90 00

    or
    - SW1 SW2 == 61 XX.

Note: We allow for 61 XX, because some systems may generate a response even if none is requested.

2. The specified file is selected.

Assertion 5.2

Purpose: To test SELECT FILE using valid parameters (explicit selection, response required).

Scenario:

1. P1 == 00.
2. P2 == 00.
3. Data Field == a valid file ID for a file on the card.
4. L_e == the maximum number of bytes expected in the data field of the response to the command *(?)*
5. A SELECT FILE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 90 00 or 61 L_e
   - Response Data Field == a string of bytes of length L_e representing the File Control Information.

Note: For systems using the T=0 communications protocol, the 61 XX response is required by ISO 7816-4.

2. The specified file is selected.

Assertion 5.3

Purpose: To test SELECT FILE using valid parameters (select parent DF, no response required)

Scenario:

1. P1 == 03.
2. P2 == 0C.
3. Data Field == empty.
4. A SELECT FILE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 90 00

   or
   - SW1 SW2 == 61 XX.

Note: For systems using the T=0 communications protocol, the 61 XX response code is required by ISO 7816-4.

2. The specified file is selected.

Assertion 5.4

Purpose: To test SELECT FILE using valid parameters (select parent DF, response required).

Scenario:

1. P1 == 03.

2. P2 == 00.

3. Data Field == empty.

4. L_e == the maximum number of bytes expected in the data field of the response to the command *(?)*

5. A SELECT FILE APDU is issued.

Expected Results:

1. The APDU returns
    - SW1 SW2 == 90 00

   or
    - SW1 SW2 == 61 XX.

   Note: For systems using the T=0 communications protocol, the 61 XX response code is required by ISO 7816-4.

2. Response Data Field == a string of bytes of length L_e representing the File Control Information.

3. The specified file is selected.

Assertion 5.5

Purpose: To test SELECT FILE using valid parameters (explicit selection, no response required) and a card in which the selected file has been deactivated.

(Is this assertion relevant enough to the GSC-IS to require testing?)

Scenario:

1. P1 == 00.

2. P2 == 00.

3. Data Field == a valid file ID for a file on the card. This file is currently deactivated.

4. A SELECT FILE APDU is issued.

Expected Results:

1. The APDU returns
    - SW1 SW2 == 62 83.

Assertion 5.6

Purpose: To test SELECT FILE using valid parameters (explicit selection, no response required) and a card in which the FCI is not formatted according to ISO 7816-4 Section 5.1.5.

(Is this assertion relevant enough to the GSC-IS to require testing?)

Scenario:

1. The FCI is not formatted according to ISO 7816-4 Section 5.1.5.
2. P1 == 00.
3. P2 == 0C.
4. Data Field == a valid file ID for a file on the card.
5. A SELECT FILE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 62 84.

Assertion 5.7

Purpose: To test SELECT FILE where the function is not supported.

The assertion is not testable.

Assertion 5.8

Purpose: To test SELECT FILE using valid parameters (explicit selection, no response required) and a card that does not contain a file identified by the specified file ID. *Note: Future versions of the Card Edge Test Suite will also include cases using select parent DF and for which response is required).*

Scenario:

1. P1 == 00.
2. P2 == 0C.
3. Data Field == a file ID that is invalid for all files on the card.
4. A SELECT FILE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2== 6A 82.

Assertion 5.9

Purpose: To test SELECT FILE using invalid parameters P1-P2.

Scenario:

1. At least one of the following is true:
   - P1 /= 00, 01, 02, or 03

- P2 /= 00 or 0C.

2. Data Field == a valid file ID for a file on the card.

3. A SELECT FILE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 6A 86.

Assertion 5.10

Purpose: To test SELECT FILE using an L_c inconsistent with P1-P2 (explicit selection, no response required) *Note: Future versions of the Card Edge Test Suite will also include cases using select parent DF and for which response is required).*

Scenario:

1. P1 == 00.

2. P2 == 0C.

3. L_c /= 02.

4. Data Field == a valid file ID for a file on the card.

5. A SELECT FILE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 6A 87.

6. SELECT MASTER FILE

CLA	00
INS	A4
P1	03
P2	00 for response required 0C for no response required
L_c	02
Data Field	file ID of Master File
L_e	Empty *(Is this always correct? If P2 == 00, shouldn't L_e contain the maximum number of bytes expected in the data field of the response to the command?)*

References:

1. GSC-IS 5.1.1.5.

Starting State for Each Assertion:

1. A card that claims to implement the GSC-IS, Version 2.1, is in a reader.

2. There is currently no file selected.

Assertion 6.1

Purpose: To test SELECT MASTER FILE using valid parameters (no response required).

Scenario:

1. P2 == 0C.

2. Data Field == the file ID for the master file on the card.

3. A SELECT MASTER FILE APDU is issued.

Expected Results:

3. The APDU returns
   - SW1 SW2 == 90 00

   or
   - SW1 SW2 == 61 XX.

Note: We allow for 61 XX, because some systems may generate a response even if none is requested.

•

1. The master file is selected.

Assertion 6.2

Purpose: To test SELECT MASTER FILE using valid parameters (response required).

Scenario:

1. P2 == 00.

2. Data Field == the file ID for the master file on the card.

3. L_e == the maximum number of bytes expected in the data field of the response to the command *(?)*

4. A SELECT MASTER FILE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 90 00 or 61 L_e
   - Response Data Field == a string of bytes of length L_e representing the File Control Information.

Note: For systems using the T=0 communications protocol, the 61 XX response is required by ISO 7816-4.

2. The master file is selected.

Assertion 6.3

Purpose: To test SELECT MASTER FILE using valid parameters (no response required) and a card in which the selected file has been deactivated.

(Is this assertion relevant enough to the GSC-IS to require testing?)

Scenario:

1. P2 == 00.

2. Data Field == the file ID for the master file on the card. This file is currently deactivated.

3. A SELECT MASTER FILE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 62 83.

Assertion 6.4

Purpose: To test SELECT MASTER FILE using valid parameters (no response required) and a card in which the FCI is not formatted according to ISO 7816-4 Section 5.1.5.

(Is this assertion relevant enough to the GSC-IS to require testing?)

Scenario:

1. The FCI is not formatted according to ISO 7816-4 Section 5.1.5.

2. P2 == 0C.

3. Data Field == the file ID for the master file on the card.

4. A SELECT MASTER FILE APDU is issued.

Expected Results:

1. The APDU returns

- SW1 SW2 == 62 84.

Assertion 6.5

Purpose: To test SELECT MASTER FILE where the function is not supported.

The assertion is not testable.

Assertion 6.6

Purpose: To test SELECT MASTER FILE using invalid parameters P1-P2.

Scenario:

1. At least one of the following is true:
    - P1 /= 00, 01, 02, or 03
    - P2 /= 00 or 0C.

2. Data Field == the file ID for the master file on the card..

3. A SELECT MASTER FILE APDU is issued.

Expected Results:

1. The APDU returns
    - SW1 SW2 == 6A 86.

Assertion 6.7

Purpose: To test SELECT MASTER FILE using an L_c inconsistent with P1-P2 (no response required).

Scenario:

1. P2 == 0C.

2. L_c /= 02.

3. Data Field == the file ID for the master file on the card.

4. A SELECT MASTER FILE APDU is issued.

Expected Results:

1. The APDU returns
    - SW1 SW2 == 6A 87.

7. UPDATE BINARY

CLA	00
INS	D6
P1	off/H
P2	off/L
L_c	number of bytes to update
Data Field	new data
L_e	empty

Note: P1P2 will be used to represent the 2 byte file offset formed by combining P1 and P2.

References:

1. GSC-IS 5.1.1.6.

Starting State for Each Assertion:

1. A card that claims to implement the GSC-IS, Version 2.1, is in a reader.

Assertion 7.1

Purpose: To test UPDATE BINARY using valid parameters.

Scenario:

1. An Elementary File on the card is currently selected.
2. P1P2 represents an offset that is within the current bounds of the selected EF.
3. L_c is a number such that the offset L_c + P1P2 is within the current bounds of the selected EF.
4. The string of L_c bytes in the selected file beginning at position P1P2 is not equal to the string of bytes of length L_c represented by the Data Field.
5. AN UPDATE BINARY APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 90 00 or 63 CX.
2. The string of L_c bytes in the selected file beginning at position P1P2 is replaced by the string in the Data Field.
3. No other changes are made to the selected file.

Assertion 7.2

Purpose: To test UPDATE BINARY where the specified number of bytes to be updated is too large to be accommodated by the selected file.

Scenario:

1. An Elementary File on the card is currently selected.

2. P1P2 represents an offset that is within the current bounds of the selected EF.

3. L_c is a number such that the offset L_c + P1P2 is outside the current bounds of the selected EF.

4. The Data Field contains a string of length $L_{c.}$

5. AN UPDATE BINARY APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 67 00.

2. No changes are made to the selected file.

Assertion 7.3

Purpose: To test UPDATE BINARY where the command is incompatible with the file structure.

This situation cannot occur in the context of UPDATE BINARY. The assertion is not testable.

Assertion 7.4

Purpose: To test UPDATE BINARY where the security status of the selected file is not satisfied.

Scenario:

1. An Elementary File on the card is currently selected.

2. P1P2 represents an offset that is within the current bounds of the selected EF.

3. L_c is a number such that the offset L_c + P1P2 is within the current bounds of the selected EF.

4. The string of L_c bytes in the selected file beginning at position P1P2 is not equal to the string of bytes of length L_c represented by the Data Field.

5. The current application has not satisfied the security status of the selected EF.

6. AN UPDATE BINARY APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 69 82.

2. No changes are made to the selected file.

Assertion 7.5

Purpose: To test UPDATE BINARY with no selected EF.

Scenario:

1. No elementary file on the card is currently selected.
2. P1P2 == 0.
3. L_c == 0.
4. The Data Field contains a string of length $L_{c.}$
5. AN UPDATE BINARY APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 69 86 or 6A 82.

Assertion 7.6

Purpose: To test UPDATE BINARY where the function is not supported.

The assertion is not testable.

Assertion 7.7

Purpose: To test UPDATE BINARY using an offset outside the selected file.

Scenario:

1. An Elementary File on the card is currently selected.
2. P1P2 represents an offset that is outside the current bounds of the selected EF.
3. L_c == 0.
4. The Data Field contains a string of length $L_{c.}$
5. AN UPDATE BINARY APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 6B 00.
2. No changes are made to the selected file.

8. EXTERNAL AUTHENTICATE

CLA	00
INS	82
P1	algorithm identifier
P2	00 for default key; 01 to 30 for key number
L_c	length of data field
Data Field	cryptogram
L_e	empty

References:
1. GSC-IS 5.1.2.1.

Starting State for Each Assertion:
1. A card that claims to implement the GSC-IS, Version 2.1, is in a reader.

2. External authentication has not been established.

Assertion 8.1

Purpose: To test EXTERNAL AUTHENTICATE using valid parameters.

Scenario:
1. P1 == a valid algorithm identifier.

2. P2 == a valid key number.

3. L_c == the length of the cryptogram in the data field.

4. Data field == a valid encrypted challenge.

5. An EXTERNAL AUTHENTICATE APDU is issued.

Expected Results:
1. The APDU returns
   - SW1 SW2 == 90 00
   - those files on the selected card subject to external authentication are opened to appropriate access.

Assertion 8.2

Purpose: To test EXTERNAL AUTHENTICATE using a bad cryptogram.

Scenario:
1. P1 == a valid algorithm identifier.

2. P2 == a valid key number.

3. L_c == the length of the cryptogram in the data field.

4. Data field == an invalid encrypted challenge.

5. An EXTERNAL AUTHENTICATE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 63 00, 63 CX, or 69 83
   - those files on the selected card subject to external authentication are not opened to appropriate access.

Assertion 8.3

Purpose: To test EXTERNAL AUTHENTICATE using a bad data field length.

Scenario:

1. P1 == a valid algorithm identifier.

2. P2 == a valid key number.

3. L_c /= the length of the cryptogram in the data field.

4. Data field == a valid encrypted challenge.

5. An EXTERNAL AUTHENTICATE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 67 00
   - those files on the selected card subject to external authentication are not opened to appropriate access.

Assertion 8.4

Purpose: To test EXTERNAL AUTHENTICATE where the referenced data is deactivated. *(Anybody know what this means? What is the referenced data and how is it deactivated?)*

(Is this assertion relevant enough to the GSC-IS to require testing?)

Scenario:

1. P1 == a valid algorithm identifier.

2. P2 == a valid key number.

3. L_c == the length of the cryptogram in the data field.

4. Data field == a valid encrypted challenge.

5. The referenced data is deactivated.

6. An EXTERNAL AUTHENTICATE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 69 84
   - those files on the selected card subject to external authentication are not opened to appropriate access.

Assertion 8.5

Purpose: To test EXTERNAL AUTHENTICATE in a context where the command is not allowed.

Scenario:

1. P1 == a valid algorithm identifier.

2. P2 == a valid key number.

3. L_c == the length of the cryptogram in the data field.

4. Data field == a valid encrypted challenge.

5. The immediately preceding command was not GET CHALLENGE.

6. An EXTERNAL AUTHENTICATE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 69 85
   - those files on the selected card subject to external authentication are not opened to appropriate access.

Assertion 8.6

Purpose: To test EXTERNAL AUTHENTICATE using invalid parameters P1-P2.

Scenario:

1. At least one of the following is true:
   - P1 is not a valid algorithm identifier
   - P2 is not a valid key number.

2. L_c == the length of the cryptogram in the data field.

3. Data field == a valid encrypted challenge.

4. An EXTERNAL AUTHENTICATE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 6A 86 or 6A 88
   - those files on the selected card subject to external authentication are not opened to appropriate access.

9. GET CHALLENGE

CLA	00
INS	84
P1	00
P2	00
L_c	empty
Data Field	empty
L_e	length in bytes of expected challenge

References:

1. GSC-IS 5.1.2.2.

Starting State for Each Assertion:

1. A card that claims to implement the GSC-IS, Version 2.1, is in a reader.

Assertion 9.1

Purpose: To test GET CHALLENGE using valid parameters.

Scenario:

1. L_e == 8.

2. A GET CHALLENGE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 90 00 or 61 L_e
   - Response Data Field == L_e bytes representing the cryptographic challenge.

Assertion 9.2

Purpose: To test GET CHALLENGE where the function is not supported.

The assertion is not testable.

Assertion 9.3

Purpose: To test GET CHALLENGE using invalid parameters P1-P2.

Scenario:

1. At least one of P1 or P2 is /= 0.

2. L_e == 8.

3. A GET CHALLENGE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 6A 86.

10. INTERNAL AUTHENTICATE

CLA	00
INS	88
P1	algorithm identifier
P2	00 for default key; 01 to 30 for key number
L_c	length of data field
Data Field	challenge
L_e	length of expected cryptogram

References:
GSC-IS 5.1.2.3.

Starting State for Each Assertion:

1. A card that claims to implement the GSC-IS, Version 2.1, is in a reader.

Assertion 10.1

Purpose: To test INTERNAL AUTHENTICATE using valid parameters.

Scenario:

1. P1 == a valid algorithm identifier.

2. P2 == a valid key number.

3. L_c == the length of the challenge in the data field.

4. Data field == an 8 byte challenge.

5. An INTERNAL AUTHENTICATE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 90 00 or 61 L_e
   - Response Data Field == L_e bytes representing the returned cryptogram.

Assertion 10.2

Purpose: To test INTERNAL AUTHENTICATE where the referenced data is deactivated. *(Anybody know what this means? What is the referenced data and how is it deactivated?)*

(Is this assertion relevant enough to the GSC-IS to require testing?)

Scenario:

1. P1 == a valid algorithm identifier.

2. P2 == a valid key number.

3. L_c == the length of the challenge in the data field.

4. Data field == an 8 byte challenge.

5. The referenced data is deactivated.

6. An INTERNAL AUTHENTICATE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 69 84.

Assertion 10.3

Purpose: To test INTERNAL AUTHENTICATE in a context where the command is not allowed.

Scenario:

1. P1 == a valid algorithm identifier.

2. P2 == a valid key number.

3. L_c == the length of the challenge in the data field.

4. Data field == an 8 byte challenge.

5. The immediately preceding command was not VERIFY.

6. An INTERNAL AUTHENTICATE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 69 85.

Assertion 10.4

Purpose: To test INTERNAL AUTHENTICATE using invalid parameters P1-P2.

Scenario:

1. At least one of the following is true:
   - P1 is not a valid algorithm identifier
   - P2 is not a valid key number.

2. L_c == the length of the challenge in the data field.

3. Data field == an 8 byte challenge.

4. An INTERNAL AUTHENTICATE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 6A 86 or 6A 88.

11. VERIFY

CLA	00
INS	20
P1	00
P2	00 for default key; 01 to 30 for key number
L_c	length of data field
Data Field	authentication data
L_e	empty

References:
1. GSC-IS 5.1.2.4.

Starting State for Each Assertion:
1. A card that claims to implement the GSC-IS, Version 2.1, is in a reader.

Assertion 11.1

Purpose: To test VERIFY using valid parameters.

Scenario:
1. P2 == a valid key number.
2. L_c == the length of the authentication data in the data field.
3. data field == valid authentication data.
4. A VERIFY APDU is issued.

Expected Results:
1. The APDU returns
   - SW1 SW2 == 90 00.

Assertion 11.2

Purpose: To test VERIFY using invalid authentication data.

Scenario:
1. P2 == a valid key number.
2. L_c == the length of the authentication data in the data field.
3. data field == invalid authentication data.
4. A VERIFY APDU is issued.

Expected Results:
1. The APDU returns
   - SW1 SW2 == 63 00, 63 CX, or 69 83.

Assertion 11.3

Purpose: To test VERIFY where the referenced data is deactivated. *(Anybody know what this means? What is the referenced data and how is it deactivated?)*

(Is this assertion relevant enough to the GSC-IS to require testing?)

Scenario:

1. P2 == a valid key number.
2. L_c == the length of the authentication data in the data field.
3. Data field == valid authentication data.
4. The referenced data is deactivated.
5. An EXTERNAL AUTHENTICATE APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 69 84.

Assertion 11.4

Purpose: To test VERIFY using invalid parameters P1-P2.

Scenario:

1. At least one of the following is true:
   - P1 /= 0
   - P2 is not a valid key number.
2. L_c == the length of the authentication data in the data field.
3. data field == valid authentication data.
4. A VERIFY APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 6A 86.

12. MANAGE SECURITY ENVIRONMENT

CLA	00
INS	22
P1	41
P2	B6
L_c	length of data field
Data Field	key reference information
L_e	empty

References:

1. GSC-IS 5.1.3.1.

Starting State for Each Assertion:

1. A card that claims to implement the GSC-IS, Version 2.1, is in a reader.

Assertion 12.1

Purpose: To test MANAGE SECURITY ENVIRONMENT using valid parameters.

Scenario:

1. L_c == the length of the key reference information in the data field.

2. data field == valid key reference information.

3. A MANAGE SECURITY ENVIRONMENT APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 90 00.

Assertion 12.2

Purpose: To test MANAGE SECURITY ENVIRONMENT when the security environment cannot be set.

Anybody know what this means and how it can be tested?

Assertion 12.3

Purpose: To test MANAGE SECURITY ENVIRONMENT using a bad data field length.

Scenario:

1. L_c /= the length of the key reference information in the data field.

2. data field == valid key reference information.

3. A MANAGE SECURITY ENVIRONMENT APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 67 00.

Assertion 12.4

Purpose: To test MANAGE SECURITY ENVIRONMENT with an invalid or missing tag, length or value in a Control Reference Data Object.

Scenario:

1. L_c == the length of the key reference information in the data field.

2. data field == key reference information containing an invalid or missing tag, length or value.

3. A MANAGE SECURITY ENVIRONMENT APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 6A 80.

Assertion 12.5

Purpose: To test MANAGE SECURITY ENVIRONMENT using invalid parameters P1-P2.

Scenario:

1. At least one of the following is true:
   - P1 /= 41
   - P2 /= B6.

2. L_c == the length of the key reference information in the data field.

3. data field == valid key reference information.

4. A MANAGE SECURITY ENVIRONMENT APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 6A 86.

13. PERFORM SECURITY OPERATION

CLA	00
INS	2A
P1	9E
P2	9A
L_c	length of data field
Data Field	message digest to sign
L_e	length of computed signature in response

References:

1. GSC-IS 5.1.3.2.

Starting State for Each Assertion:

1. A card that claims to implement the GSC-IS, Version 2.1, is in a reader.

Assertion 13.1

Purpose: To test PERFORM SECURITY OPERATION using valid parameters.

Scenario:

1. L_c == the length of the string in the data field.

2. data field == a valid message to sign.

3. A PERFORM SECURITY OPERATION APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 90 00 or 61 L_e
   - Response Data Field == L_e bytes representing the computed signature.

Assertion 13.2

Purpose: To test PERFORM SECURITY OPERATION using an invalid L_c.

Scenario:

1. L_c /= the length of the string in the data field.

2. data field == a valid message to sign.

3. A PERFORM SECURITY OPERATION APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 67 00.

Assertion 13.3

Purpose: To test PERFORM SECURITY OPERATION using an invalid file type.
(Anybody know what this means? What file are they talking about?)

(Is this assertion relevant enough to the GSC-IS to require testing?)

Scenario:

1. L_c == the length of the string in the data field.

2. data field == a valid message to sign.

3. File is invalid *(???)*.

4. A PERFORM SECURITY OPERATION APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 69 81.

Assertion 13.4

Purpose: To test PERFORM SECURITY OPERATION where the previous operation was not MANAGE SECURITY ENVIRONMENT.

Scenario:

1. L_c == the length of the string in the data field.

2. data field == a valid message to sign.

3. The immediately preceding command was not MANAGE SECURITY ENVIRONMENT.

4. A PERFORM SECURITY OPERATION APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 69 85.

Assertion 13.5

Purpose: To test PERFORM SECURITY OPERATION with a missing message digest.

Scenario:

1. L_c == 0.

2. data field == empty.

3. A PERFORM SECURITY OPERATION APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 69 87.

Assertion 13.6

Purpose: To test PERFORM SECURITY OPERATION with an invalid message digest.

Scenario:

1. L_c == 0.

2. data field == an invalid message digest.

3. A PERFORM SECURITY OPERATION APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 69 88.

Assertion 13.7

Purpose: To test PERFORM SECURITY OPERATION using invalid parameters P1-P2.

Scenario:

1. At least one of the following is true:
   - P1 /= 9E
   - P2 /= 9A.

2. L_c == the length of the string in the data field.

3. data field == a valid message to sign.

4. A PERFORM SECURITY OPERATION APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 6A 86.

Assertion 13.8

Purpose: To test PERFORM SECURITY OPERATION specifying an incorrect length for the response string.

Scenario:

1. L_c == the length of the string in the data field.

2. data field == a valid message to sign.

3. L_e /= length of the computed signature.

4. A PERFORM SECURITY OPERATION APDU is issued.

Expected Results:

1. The APDU returns
   - SW1 SW2 == 6C XX.